

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

Commissioner
 US Department of Commerce
 United States Patent and Trademark
 Office, PCT
 2011 South Clark Place Room
 CP2/5C24
 Arlington, VA 22202
 ETATS-UNIS D'AMERIQUE
 en sa qualité d'office élu

Date d'expédition (jour/mois/année) 01 décembre 2000 (01.12.00)	Référence du dossier du déposant ou du mandataire GEM0630
Demande internationale no PCT/FR00/00130	Date de priorité (jour/mois/année) 17 février 1999 (17.02.99)
Date du dépôt international (jour/mois/année) 20 janvier 2000 (20.01.00)	
Déposant CORON, Jean-Sébastien etc	

1. L'office désigné est avisé de son élection qui a été faite:



dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

14 septembre 2000 (14.09.00)



dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection ☒ a été faite

n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse no de télécopieur: (41-22) 740.14.35	Fonctionnaire autorisé R. Forax no de téléphone: (41-22) 338.83.38
--	--

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FR 00/00130

A. CLASSIFICATION OF SUBJECT MATTER IPC 7 : H04L 9/06 International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC 7 : H04L, G06F Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practical, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MIYAGUCHI S: "SECRET KEY CIPHERS THAT CHANGE THE ENCIPHERMENT ALGORITHM UNDER THE CONTROL OF THE KEY" NTT REVIEW, Vol. 6, no.4, 01 July 1994 (01.07.94), pages 85-90, XP000460342 The whole document ---	I-10
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C. <input checked="" type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 12 April 2000 (12.04.00)		Date of mailing of the international search report 19 April 2000 (19.04.00)
Name and mailing address of the ISR European Patent Office		Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International Application No
PCT/FR 00/00130

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2672402	A	07-08-1992	NONE

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No

PCT/FR 00/00130

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

CIB 7 H04L9/06

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>MIYAGUCHI S: "SECRET KEY CIPHERS THAT CHANGE THE ENCIPHERMENT ALGORITHM UNDER THE CONTROL OF THE KEY"</p> <p>NTT REVIEW, vol. 6, no. 4, 1 juillet 1994 (1994-07-01), pages 85-90, XP000460342</p> <p>le document en entier</p> <p style="text-align: center;">---</p> <p style="text-align: center;">-/--</p>	1-10

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- "E" document antérieur, mais publié à la date de dépôt international ou après cette date
- "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"Z" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

12 avril 2000

Date d'expédition du présent rapport de recherche internationale

19/04/2000

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Gautier, L

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No

PCT/FR 00/00130

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
FR 2672402 A	07-08-1992	AUCUN	

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire GEM0630	POUR SUITE A DONNER voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 00/ 00130	Date du dépôt international (jour/mois/année) 20/01/2000	(Date de priorité (la plus ancienne) (jour/mois/année) 17/02/1999
Déposant GEMPLUS et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.



Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. Base du rapport

a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.



la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

b. En ce qui concerne les **séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :



contenu dans la demande internationale, sous forme écrite.



déposée avec la demande internationale, sous forme déchiffrable par ordinateur.



remis ultérieurement à l'administration, sous forme écrite.



remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.



La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.



La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2.



Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (voir le cadre I).

3.



Il y a absence d'unité de l'invention (voir le cadre II).

4. En ce qui concerne le **titre**,



le texte est approuvé tel qu'il a été remis par le déposant.



Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne l'**abrégé**,



le texte est approuvé tel qu'il a été remis par le déposant



le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n°



suggérée par le déposant.



parce que le déposant n'a pas suggéré de figure.



parce que cette figure caractérise mieux l'invention.

3



Aucune des figures n'est à publier.

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

CIB 7 H04L9/06

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	MIYAGUCHI S: "SECRET KEY CIPHERS THAT CHANGE THE ENCIPHERMENT ALGORITHM UNDER THE CONTROL OF THE KEY" NTT REVIEW, vol. 6, no. 4, 1 juillet 1994 (1994-07-01), pages 85-90, XP000460342 le document en entier --- -/--	1-10

☒ Voir la suite du cadre C pour la fin de la liste des documents☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

- "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- "E" document antérieur, mais publié à la date de dépôt international ou après cette date
- "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

- "T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
- "X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- "Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
- "&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

12 avril 2000

Date d'expédition du présent rapport de recherche internationale

19/04/2000

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
 Fax: (+31-70) 340-3016

Fonctionnaire autorisé

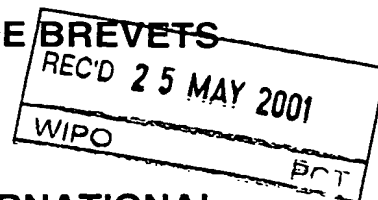
Gautier, L

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>YI X ET AL: "A METHOD FOR OBTAINING CRYPTOGRAPHICALLY STRONG 8X8 S-BOXES" IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, PHOENIX, ARIZONA, NOV. 3 - 8, 1997, vol. 2, 3 novembre 1997 (1997-11-03), pages 689-693, XP000737626 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS abrégé colonne 1, ligne 13 - ligne 29 colonne 2, ligne 6 - ligne 18 colonne 3, ligne 1 - colonne 5, ligne 1 ---</p>	1-5
A	<p>FR 2 672 402 A (GEMPLUS CARD INT) 7 août 1992 (1992-08-07) abrégé page 1, ligne 4 - ligne 12 page 3, ligne 19 - ligne 23 figure 1 revendication 1 -----</p>	11,12

Information on patent family members

PCT/FR 00/00130

Form PCT/ISA/210 (patent family annex) (July 1992)



Référence du dossier du déposant ou du mandataire GEM0630	POUR SUITE A DONNER voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR00/00130	Date du dépôt international (jour/mois/année) 20/01/2000	Date de priorité (jour/mois/année) 17/02/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/06		
Déposant GEMPLUS et al.		


1. Le présent rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.
2. Ce RAPPORT comprend 8 feuilles, y compris la présente feuille de couverture.

☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

Ces annexes comprennent 25 feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

- I ☒ Base du rapport
- II ☐ Priorité
- III ☒ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
- IV ☐ Absence d'unité de l'invention
- V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- VI ☐ Certains documents cités
- VII ☐ Irrégularités dans la demande internationale
- VIII ☒ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale 14/09/2000	Date d'achèvement du présent rapport 22.05.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international:  Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Dechmann, J-L N° de téléphone +49 89 2399 8826



RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/00130

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

Description, pages:

1-15 reçue(s) le 09/03/2001 avec la lettre du 05/03/2001

Revendications, N°:

1-9 reçue(s) le 09/03/2001 avec la lettre du 05/03/2001

Dessins, feuilles:

1/7-7/7 reçue(s) le 09/03/2001 avec la lettre du 05/03/2001

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

- ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
- ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
- ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listage des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

**RAPPORT D'EXAMEN
PRÉLIMINAIRE INTERNATIONAL**

Demande internationale n° PCT/FR00/00130

- ☐ de la description, pages :
 - ☐ des revendications, n°s :
 - ☐ des dessins, feuilles :
5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

III. Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle

1. La question de savoir si l'objet de l'invention revendiquée semble être nouveau, impliquer une activité inventive (ne pas être évident) ou être susceptible d'application industrielle n'a pas été examinée pour ce qui concerne :

- ☐ l'ensemble de la demande internationale.
- ☒ les revendications n°s 6, 9.

parce que :

- ☐ la demande internationale, ou les revendications n°s en question, se rapportent à l'objet suivant, à l'égard duquel l'administration chargée de l'examen préliminaire international n'est pas tenue effectuer un examen préliminaire international (*préciser*) :
 - ☒ la description, les revendications ou les dessins (*en indiquer les éléments ci-dessous*), ou les revendications n°s 6, 9 en question ne sont pas clairs, de sorte qu'il n'est pas possible de formuler une opinion valable (*préciser*) :
voir feuille séparée
 - ☐ les revendications, ou les revendications n°s en question, ne se fondent pas de façon adéquate sur la description, de sorte qu'il n'est pas possible de formuler une opinion valable.
 - ☐ il n'a pas été établi de rapport de recherche internationale pour les revendications n°s en question.
2. Le listage des séquences de nucléotides ou d'acides aminés n'est pas conforme à la norme prévue dans l'annexe C des instructions administratives, de sorte qu'il n'est pas possible d'effectuer un examen préliminaire international significatif :
- ☐ le listage présenté par écrit n'a pas été fourni ou n'est pas conforme à la norme.
 - ☐ le listage sous forme déchiffrable par ordinateur n'a pas été fourni ou n'est pas conforme à la norme.

**RAPPORT D'EXAMEN
PRÉLIMINAIRE INTERNATIONAL**

Demande internationale n° PCT/FR00/00130

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui : Revendications 1-5,7-8
	Non : Revendications
Activité inventive	Oui : Revendications 1-5,7-8
	Non : Revendications
Possibilité d'application industrielle	Oui : Revendications 1-5,7-8
	Non : Revendications

**2. Citations et explications
voir feuille séparée**

VIII. Observations relatives à la demande internationale

Les observations suivantes sont faites au sujet de la clarté des revendications, de la description et des dessins et de la question de savoir si les revendications se fondent entièrement sur la description :
voir feuille séparée

III. Non-Formulation d'opinion quant à la nouveauté, l'activité inventive et l'application industrielle

Voir section VIII concernant les revendications 6 et 9.

V. Déclaration motivée selon la règle 66.2.a)ii) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

I

Les documents (D) suivants ont été pris en compte pour l'établissement du rapport d'examen préliminaire:

- D1: NTT REVIEW, vol. 6, no. 4, 1 juillet 1994, pages 85-90, MIYAGUCHI S:
"SECRET KEY CIPHERS THAT CHANGE THE ENCIPHERMENT
ALGORITHM UNDER THE CONTROL OF THE KEY", XP000460342
- D2: INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE
GLOBAL TELECOMMUNICATIONS CONFERENCE, PHOENIX, ARIZONA,
NOV. 3 - 8, 1997, vol. 2, 3 novembre 1997, pages 689-693, YI X ET AL: "A
METHOD FOR OBTAINING CRYPTOGRAPHICALLY STRONG 8X8 S-
BOXES", XP000737626
- D3: FR-A-2 672 402

II

La présente invention concerne un procédé de contre-mesure contre des attaques par analyse différentielle de consommation de courant (ou attaques DPA: Differential

Power Analysis) dans un composant électronique mettant en oeuvre un algorithme de cryptographie à clé secrète.

Il existe de nombreux algorithmes à clés secrète pour l'exécution desquels le microprocesseur doit effectuer à certains moment des manipulations de données bit par bit. Notamment, les algorithmes comprennent généralement des permutations qui nécessitent de telles manipulations par le microprocesseur.

En analysant la consommation de courant lors de l'exécution de ces manipulations bit par bit, il est possible de retrouver la valeur de certains bits au moins de la donnée manipulée. La connaissance de cette donnée peut fournir des informations sur des résultats intermédiaires obtenus lors de l'exécution de l'algorithme de chiffrement, qui à leur tour peuvent permettre de retrouver une partie au moins des bits de la clé secrète utilisée.

La présente invention a pour objet de protéger les données sur lesquelles on effectue des manipulations bit par bit, en leur appliquant une contre-mesure, c'est à dire un brouillage, en sorte que l'analyse de la consommation de courant lors de la manipulation de cette donnée ne révèle aucune information sur cette donnée.

L'invention consiste, pour une opération ou une suite d'opérations appliquée sur une donnée d'entrée et comprenant au moins une manipulation bit par bit, à tirer au préalable une première donnée aléatoire de même taille que la première donnée, à calculer une deuxième donnée aléatoire en effectuant un OU exclusif entre la première donnée aléatoire et la donnée d'entrée, et à appliquer successivement l'opération ou la suite d'opérations à la première donnée aléatoire et à la deuxième donnée aléatoire. De cette manière, l'opération ou la suite d'opérations ne manipule que des données aléatoires en sorte qu'il n'est plus possible de mettre en oeuvre une attaque DPA. Pour retrouver la donnée de sortie correspondent à l'application de la suite d'étapes sur la donnée d'entrée, il suffit de calculer le OU exclusif entre le premier et le deuxième résultats aléatoires.

Le document D1 concerne une résolution à un problème mathématique qui évite les attaques à message et chiffrées connues. La méthode décrite modifie la sous-partie de la clé dans l'algorithme, de n'importe quel algorithme à clé secrète. La technologie décrite dans ce document consiste à effectuer des rotations de données et aussi de substitution de données.

Ainsi, la présente invention se distingue du document D1 en ce qu'elle ne modifie la structure de l'algorithme, ni ses entrées, ni ses sorties de données. L'opération XOR utilisée permet de masquer les données avec un paramètre aléatoire.

Le document D2, concerne une proposition d'amélioration des S BOX dans l'algorithme DES standard destinée à améliorer la sécurisation sur un plan cryptanalyse, c'est à dire en mathématique, mais pas en cryptographie physique.

L'invention se distingue également du document D2 en ce qu'elle aborde les problèmes de cryptographies physique c'est à dire qu'elle propose de résoudre des problèmes de mise en oeuvre par apparition d'effets secondaires ; par ailleurs elle ne concerne pas les S BOX mais aborde les problèmes de sécurisation lors des compressions, permutations, expansions des données.

Le document D3, concerne un procédé et dispositif utilisant l'algorithme standard DES pour construire un générateur de nombres aléatoires. L'algorithme DES est un algorithme à clé secrète avec des données comme par exemple un compteur destiné à générer en sortie un résultat qui peut être assimilé à un nombre aléatoire, résultat situé à l'extérieur du DES.

L'invention se distingue du document D3 en ce qu'elle utilise un nombre aléatoire à l'intérieur de l'algorithme DES pour sécuriser l'exécution du DES contre tous types d'attaques.

Une activité inventive est donc reconnue. Les revendications 1-5, 7-8 remplissent donc les exigences de l'Article 33(3) PCT.

VIII. Observations relatives à la demande internationale

1. La syntaxe de la revendication 6 n'est pas claire (Article 6 PCT). La première phrase ne comprend pas de verbe. Le Demandeur veut-il dire "à chaque tour où une opération de OU exclusif entre la sous-clé et une donnée d'entrée **est utilisée**, cette opération est remplacée par les donnée suivantes..."?

2. La revendication 9 n'est pas claire (Article 6 PCT) en ce qu'elle mentionne qu'une valeur aléatoire est générée tout en restant silencieuse sur ce qui est fait ensuite avec cette variable aléatoire (calcul d'une deuxième donnée aléatoire, exécution d'une opération, calcul d'une donnée de sortie, etc...).
L'invention ne consiste sûrement pas seulement en la génération d'une variable aléatoire mais plutôt dans les moyens qui ensuite l'utilisent afin de lutter contre une attaque DPA.
La revendication d'appareil n'est donc pas claire en ce qu'elle ne contient pas toutes les caractéristiques techniques essentielles nécessaires à la définition de l'invention (Article 6 en combinaison avec la Règle 6.3(b) PCT).
De plus, la formulation "de taille voulue" est relative et n'a pas de signification précise (voir Directives PCT, Chap. III-4.5).

3. Les revendications 5 et 6 ne sont pas claires en ce que la formulation "caractérisé en ce que" ne se situe pas juste après "Procédé... selon la revendication...". En effet ces deux revendications dépendent indirectement de la revendication 1 qui a déjà un préambule et une partie caractérisante. Les revendications 5 et 6 combinées avec la revendication 1 ont donc deux préambules et deux parties caractérisantes laissant ainsi subsister un doute quant à l'étendue de leur protection.

**PROCEDE DE CONTRE-MESURE DANS UN COMPOSANT
ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE
CRYPTOGRAPHIE A CLE SECRETE**

La présente invention concerne un procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme de cryptographie à clé secrète. Ils sont utilisés dans des applications où l'accès à des services ou à des données est sévèrement contrôlé. De tels composants ont une architecture formée autour d'un microprocesseur et de mémoires, dont une mémoire programme qui contient la clé secrète.

Ces composants sont notamment utilisés dans les cartes à puce, pour certaines applications de celles-ci. Ce sont par exemple des applications d'accès à certaines banques de données, des applications bancaires, des applications de télé-péage, par exemple pour la télévision, la distribution d'essence ou encore le passage de péages d'autoroutes.

Ces composants ou ces cartes mettent donc en oeuvre un algorithme de cryptographie à clé secrète, dont le plus connu est l'algorithme DES (pour *Data Encryption Standard* dans la littérature anglo-saxonne). D'autres algorithmes à clé secrète existent, comme l'algorithme RC5 ou encore l'algorithme COMP128. Cette liste n'est bien sûr pas exhaustive.

De manière générale et succincte, ces algorithmes ont pour fonction de calculer un message chiffré à partir d'un message appliqué en entrée (à la carte) par un système hôte (serveur, distributeur bancaire...) et de la clé secrète contenue dans la carte, et de fournir en retour au système hôte ce message chiffré, ce qui permet par exemple au système hôte d'authentifier le composant ou la carte, d'échanger des données...

Les caractéristiques des algorithmes de cryptographie à clé secrète sont connues : calculs effectués, paramètres utilisés. La seule inconnue est la clé secrète contenue en mémoire programme. Toute la sécurité de ces algorithmes de cryptographie tient dans cette clé secrète contenue dans la carte et inconnue du monde extérieur à cette carte. Cette clé secrète ne peut être déduite de la seule connaissance du message appliqué en entrée et du message chiffré fourni en retour.

Or il est apparu que des attaques externes, basées sur les consommations de courant ou une analyse différentielle de consommation en courant lorsque le microprocesseur d'une carte est en train de dérouler l'algorithme de cryptographie pour calculer un message chiffré, permettent à des tiers mal intentionnés de trouver la clé secrète contenue dans cette carte. Ces attaques sont appelées attaques DPA, acronyme anglo-saxon pour *Differential Power Analysis*.

Le principe de ces attaques DPA repose sur le fait que la consommation en courant du microprocesseur exécutant des instructions varie selon la donnée manipulée.

Notamment, quand une instruction exécutée par le microprocesseur nécessite une manipulation d'une donnée bit par bit, on a deux profils de courant différents selon que ce bit vaut "1" ou "0". Typiquement, si le microprocesseur manipule un "0", on a à cet instant d'exécution une première amplitude du courant consommé et si le microprocesseur manipule un "1", on a une deuxième amplitude du courant consommé, différente de la première.

Ainsi l'attaque DPA exploite la différence du profil de consommation en courant dans la carte pendant l'exécution d'une instruction suivant la valeur du bit manipulé. D'une manière simplifiée, la conduite d'une

attaque DPA consiste à identifier une ou des périodes particulières du déroulement de l'algorithme comprenant l'exécution d'au moins une instruction manipulant des données bit par bit; à relever un très grand nombre N
5 de courbes de consommation en courant pendant cette ou ces périodes, une courbe par message différent sur lequel on applique l'algorithme; à prédire, pour chaque courbe, la valeur prise par un bit de la donnée pour une hypothèse sur une sous-clé, c'est à dire sur une
10 partie au moins de la clé secrète, qui permet de faire la prédiction ; et à effectuer un tri des courbes selon la fonction de sélection booléenne correspondante : on obtient un premier paquet de courbes pour lesquelles la prédiction vaut "1" et un deuxième paquet de courbes
15 pour lesquelles la prédiction vaut "0". En effectuant une analyse différentielle de la consommation moyenne en courant entre les deux paquets de courbes obtenus, on obtient un signal d'information DPA(t). Si l'hypothèse de sous-clé n'est pas juste, chaque paquet
20 comprend en réalité autant de courbes correspondant à la manipulation d'un "1" que de courbes manipulant un "0". Les deux paquets sont donc équivalents en terme de consommation en courant et le signal d'information est sensiblement nul. Si l'hypothèse de sous-clé est juste,
25 un paquet comprend réellement les courbes correspondant à la manipulation d'un "0" et l'autre paquet comprend réellement les courbes correspondant à la manipulation d'un "0" : le signal d'information DPA(t) obtenu n'est pas nul : il comprend des pics de consommation
30 correspondant à la manipulation par le microprocesseur du bit sur lequel on a basé le tri. Ces pics ont une amplitude correspondant à la différence de consommation par le microprocesseur selon qu'il manipule un "1" ou un "0". Ainsi, de proche en proche, il est possible de
35 découvrir tout ou partie de la clé secrète contenue dans un composant électronique.

Il existe de nombreux algorithmes à clé secrète pour l'exécution desquels le microprocesseur doit effectuer à certains moments des manipulations de données bit par bit.

5 Notamment, les algorithmes comprennent généralement des permutations qui nécessitent de telles manipulations par le microprocesseur. En analysant la consommation de courant lors de l'exécution de ces manipulations bit par bit, il est possible de retrouver
10 la valeur de certains bits au moins de la donnée manipulée. La connaissance de cette donnée peut fournir des informations sur des résultats intermédiaires obtenus lors de l'exécution de l'algorithme de chiffrement, qui à leur tour peuvent permettre de
15 retrouver une partie au moins des bits de la clé secrète utilisée.

Trois documents s'approchant de l'invention tout en s'en démarquant sont cités ci-dessous.

20 Le premier document « NTT REVIEW, Vol.6, no.4, du 1 juillet 1997, pages 85-90, MIYAGUCHI S : « SECRET KEY CIPHERS THAT CHANGE THE ENCIPHERMENT ALGORITHM UNDER THE CONTROL OF THE KEY », XP000460342 », noté D1, concerne une résolution à un problème mathématique qui évite les attaques à message et chiffrées connues. La
25 méthode décrite modifie le « key schedule », traduit par « sous-partie de la clé dans l'algorithme », de n'importe quel algorithme à clé secrète. Cependant, cette méthode ne s'adresse plus à l'algorithme standard DES, algorithme à clé secrète bien connue. La
30 technologie décrite dans ce document consiste à effectuer des rotations de données et aussi de substitution de données.

35 Le second document « INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, PHOENIX, ARIZONA, NOV.3-8, 1997, vol.2, 3 novembre 1997, pages 689-693, YI X ET AL : "A METHOD

FOR OBTAINING CRYPTOGRAPHICALLY STRONG 8X8 S-BOXES",
XP000737626 », noté D2, concerne une proposition
d'amélioration des S BOX dans l'algorithme DES standard
destinée à améliorer la sécurisation sur un plan
5 cryptanalyse, c'est à dire en mathématique, mais pas en
cryptographie physique.

Le troisième document « FR-A-2 672 402 », noté D3,
concerne un procédé et dispositif utilisant
l'algorithme standard DES pour construire un générateur
10 de nombres aléatoires. L'algorithme DES est un
algorithme à clé secrète avec des données comme par
exemple un compteur destiné à générer en sortie un
résultat qui peut être assimilé à un nombre aléatoire,
résultat situé à l'extérieur du DES.

15 La présente invention a pour objet de protéger les
données sur lesquelles on effectue des manipulations
bit par bit, en leur appliquant une contre-mesure,
c'est à dire un brouillage, en sorte que l'analyse de
la consommation de courant lors de la manipulation de
20 cette donnée ne révèle aucune information sur cette
donnée : le signal d'information DPA(t) sera toujours
nul quelque soit les hypothèses de sous-clé ou de clé
effectuées dans les attaques DPA.

Telle que revendiquée, l'invention concerne un
25 procédé de contre-mesure dans un composant électronique
mettant en oeuvre un algorithme cryptographique à clé
secrète K.

Selon l'invention, le procédé de contre-mesure
consiste, pour une opération ou une suite d'opérations
30 appliquée sur une donnée d'entrée et comprenant au
moins une manipulation bit par bit, à tirer au
préalable une première donnée aléatoire de même taille
que la première donnée, à calculer une deuxième donnée
aléatoire en effectuant un OU exclusif entre la
35 première donnée aléatoire et la donnée d'entrée, et à
appliquer successivement l'opération ou la suite

d'opérations à la première donnée aléatoire et à la deuxième donnée aléatoire.

De cette manière, l'opération ou la suite d'opérations ne manipule que des données aléatoires en sorte qu'il n'est plus possible de mettre en oeuvre une
5 attaque DPA.

Pour retrouver la donnée de sortie correspondant à l'application de la suite d'étapes sur la donnée d'entrée, il suffit de calculer le OU exclusif entre le
10 premier et le deuxième résultats aléatoires.

Dans un premier mode d'application de ce procédé de contre-mesure, l'opération ou la suite d'opérations porte sur une donnée calculée à partir du message à chiffrer.

15 Dans un deuxième mode d'application du procédé de contre-mesure selon l'invention, on applique ce procédé à des opérations portant directement sur la clé secrète et fournissant pour chaque tour de l'algorithme la sous-clé à utiliser.

20 Dans ce mode d'application du procédé de contre-mesure selon l'invention, on prévoit d'effectuer une première suite d'étapes selon le procédé indiqué plus haut en sorte que l'on obtient une première sous-clé aléatoire et une deuxième sous-clé aléatoire.

25 Dans cette variante, au lieu de calculer la sous-clé vraie pour le tour considéré, on utilise ces sous-clés aléatoires, en sorte que la sous-clé vraie de chaque tour n'apparaît plus en clair : on ne manipule que des sous-clé aléatoires.

30 Ainsi, la présente invention se distingue d'abord du document D1 en ce qu'elle concerne uniquement le DES sans modifier sa structure, ni ses entrées, ni ses sorties de données. L'opération XOR utilisée décrite ci-dessous permet de masquer les données avec un
35 paramètre aléatoire.

Elle se distingue également du document D2 en ce qu'elle aborde les problèmes de cryptographies physique c'est à dire qu'elle propose de résoudre des problèmes de mise en œuvre par apparition d'effets secondaires ;
5 par ailleurs elle ne concerne pas les S BOX mais aborde les problèmes de sécurisation lors des compressions, permutations, expansions des données (cf figure 1 ci-dessous décrite).

Enfin, elle se distingue du document D3 en ce
10 qu'elle utilise un nombre aléatoire à l'intérieur de l'algorithme DES pour sécuriser l'exécution du DES contre tous types d'attaques.

D'autres caractéristiques et avantages de l'invention sont détaillés dans la description suivante
15 faite à titre indicatif et nullement limitatif et en référence aux dessins annexés, dans lesquels :

- les figures 1 et 2 sont des organigrammes détaillés des premiers et derniers tours de l'algorithme DES;

- 20 - la figure 3 représente schématiquement le procédé de contre-mesure selon l'invention appliqué à une opération effectuant une manipulation de donnée bit par bit.

- 25 - la figure 4 représente un premier mode d'application du procédé de contre-mesure selon l'invention dans l'exécution de l'algorithme DES;

- la figure 5 représente schématiquement la fin d'exécution de l'algorithme DES ;

- 30 - la figure 6 représente schématiquement deuxième mode d'application du procédé selon l'invention sur les opérations de l'algorithme DES manipulant la clé secrète; et

- 35 - la figure 7 représente un organigramme détaillé de l'algorithme DES dans une application du procédé de contre-mesure correspondant au schéma de la figure 5; et

- la figure 8 représente un schéma-bloc d'une carte à puce dans laquelle on peut mettre en oeuvre un procédé de contre-mesure selon l'invention.

L'algorithme cryptographique à clé secrète DES (dans la suite on parlera plus simplement du DES ou de l'algorithme DES) comporte 16 tours de calcul, notés T1 à T16, comme représenté sur les figures 1 et 2.

Le DES débute par une permutation initiale IP sur le message d'entrée M (figure 1). Le message d'entrée M est un mot f de 64 bits. Après permutation, on obtient un mot e de 64 bits, que l'on coupe en deux pour former les paramètres d'entrée L0 et R0 du premier tour (T1). L0 est un mot d de 32 bits contenant les 32 bits de poids forts du mot e. R0 est un mot h de 32 bits contenant les 32 bits de poids faibles du mot e.

La clé secrète K, qui est un mot q de 64 bits subit elle-même une permutation et une compression pour fournir un mot r de 56 bits.

Le premier tour comprend une opération EXP PERM sur le paramètre R0, consistant en une expansion et une permutation, pour fournir en sortie un mot l de 48 bits.

Ce mot l est combiné à un paramètre K1, dans une opération de type OU EXCLUSIF notée XOR, pour fournir un mot b de 48 bits. Le paramètre K1 qui est un mot m de 48 bits est obtenu du mot r par un décalage d'une position (opération notée SHIFT sur les figures 1 et 2) fournissant un mot p de 48 bits; sur lequel on applique une opération comprenant une permutation et une compression (opération notée COMP PERM).

Le mot b est appliqué à une opération notée SBOX, en sortie de laquelle on obtient un mot a de 32 bits. Cette opération particulière consiste à fournir une donnée de sortie a prise dans une table de constantes TC0 en fonction d'une donnée d'entrée b.

Le mot a subit une permutation P PERM, donnant en sortie le mot c de 32 bits.

Ce mot c est combiné au paramètre d'entrée L0 du premier tour T1, dans une opération logique de type OU EXCLUSIF, notée XOR, qui fournit en sortie le mot g de 32 bits.

Le mot h (=R0) du premier tour fournit le paramètre d'entrée L1 du tour suivant (T2) et le mot g du premier tour fournit le paramètre d'entrée R1 du tour suivant. Le mot p du premier tour fournit l'entrée r du tour suivant.

Les autres tours T2 à T16 se déroulent de façon similaire, excepté en ce qui concerne l'opération de décalage SHIFT qui se fait sur une ou deux positions selon les tours considérés.

Chaque tour T_i reçoit ainsi en entrée les paramètres L_{i-1} , R_{i-1} et r et fournit en sortie les paramètres L_i et R_i et r pour le tour suivant T_{i+1} .

En fin d'algorithme DES (figure 5), le message chiffré est calculé à partir des paramètres L16 et R16 fournis par le dernier tour T16.

Ce calcul du message chiffré C comprend en pratique les opérations suivantes :

- formation d'un mot e' de 64 bits en inversant la position des mots L16 et R16, puis en les concaténant;
- application de la permutation IP^{-1} inverse de celle de début de DES, pour obtenir le mot f' de 64 bits formant le message chiffré C.

On voit que cet algorithme comprend de nombreuses opérations manipulant les données bit par bit, comme les opération de permutation.

Selon le procédé de contre-mesure selon l'invention, on applique une contre-mesure logicielle lorsque le microprocesseur qui calcule le message chiffré effectue une manipulation bit par bit. De cette manière, le traitement statistique et la fonction de

sélection booléenne de l'attaque DPA appliqué aux courbes de consommation de courant ne fournit plus aucune information : le signal $DPA(t)$ reste nul quelle que soit les hypothèses de sous-clé effectuées.

5 La contre-mesure logicielle selon l'invention consiste ainsi à rendre imprédictible chacun des bits manipulés par le microprocesseur.

Le principe de cette contre-mesure est représenté sur la figure 3.

10 Soit une donnée d'entrée D .

Soit une opération OPN à calculer sur cette donnée d'entrée D , dont le résultat est noté $OPN(D)$. Cette opération OPN nécessite une manipulation bit par bit de la donnée d'entrée D par le microprocesseur; il s'agit
15 par exemple d'une permutation.

Selon l'invention, au lieu d'appliquer l'opération OPN sur la donnée d'entrée D pour calculer le résultat $OPN(D)$ de l'opération, on effectue les différentes étapes suivantes :

20 - tirage d'une valeur aléatoire pour une première donnée aléatoire U , de même taille que la donnée d'entrée D (par exemple, 32 bits) ;

25 - calcul d'une deuxième donnée aléatoire V en effectuant un OU exclusif entre la donnée d'entrée et la première donnée aléatoire : $V = D \text{ XOR } U$;

30 - calcul de l'opération OPN sur la première donnée aléatoire U , donnant un premier résultat aléatoire $OPN(U)$;

35 - calcul de l'opération OPN sur la deuxième donnée aléatoire V , donnant un deuxième résultat aléatoire $OPN(V)$;

- calcul du résultat $OPN(D)$ en effectuant un OU exclusif entre le premier et le deuxième résultats aléatoires : $OPN(D) = OPN(U) \text{ XOR } OPN(V)$.

On peut aussi bien appliquer ce procédé à une seule opération qu'à une suite d'opérations.

Un premier mode d'application du procédé de contre-mesure selon l'invention concerne des opérations sur des données calculées à partir du message (M) sur lequel on applique l'algorithme. La donnée d'entrée D est dans ce cas une donnée calculée à partir du message M.

Dans un exemple pratique de ce premier mode d'application à l'algorithme DES représenté sur la figure 4, on applique ce procédé d'une part à l'opération EXP PERM et d'autre part à l'opération P PERM, qui comprennent toutes deux une permutation nécessitant une manipulation bit par bit de la donnée d'entrée.

Sur la figure on note $CM(EXP\ PERM)$ et $CM(P\ PERM)$ l'application de cette contre-mesure sur ces opérations.

La contre-mesure logicielle selon l'invention consiste alors à effectuer à la place de chaque opération P PERM et EXP PERM les opérations $CM(EXP\ PERM)$ et $CM(P\ PERM)$ selon la séquence de calcul décrite à la figure 3, en utilisant une variable aléatoire U. Comme chaque tour de l'algorithme comprend une opération EXP PERM et une opération P PERM, on peut appliquer cette contre-mesure dans chacun des tours du DES.

L'expérience montre que ce sont les trois premiers tours et les trois derniers tours qui permettent les attaques DPA. Après, il devient très difficile voire impossible de prédire les bits.

Aussi, une mise en oeuvre moins coûteuse en temps de calcul d'un procédé de contre-mesure selon l'invention consiste à ne l'appliquer qu'à ces trois premiers et trois derniers tours du DES.

Différentes variantes d'application du procédé de contre-mesure selon l'invention concerne le tirage d'une valeur aléatoire pour la première donnée

aléatoire U. Selon que l'on dispose de beaucoup de temps de calcul ou pas, on peut tirer une nouvelle valeur aléatoire à chaque fois, pour chacune des opérations ou suite d'opérations pour lesquelles le procédé de contre-mesure selon l'invention est mis en oeuvre.

Sur la figure 4, c'est ainsi que, pour l'opération CM(EXP PERM), on tire une valeur u1 pour la donnée aléatoire U, et, pour l'opération CM(P PERM), on tire une autre valeur u2 pour la donnée aléatoire U.

Ou bien, on peut tirer une nouvelle valeur aléatoire pour chaque tour de l'algorithme, ou encore une seule valeur aléatoire en début d'algorithme.

La mise en oeuvre du procédé de contre-mesure selon l'invention dépend principalement des applications concernées, selon que l'on peut consacrer beaucoup de temps supplémentaire à la contre-mesure ou pas.

Un deuxième mode d'application du procédé de contre-mesure selon l'invention est représenté sur la figure 6. Il concerne plus particulièrement les opérations de calcul appliquées à la clé secrète K pour fournir chacune des sous-clés Ki utilisées dans les tours de l'algorithme. Dans l'exemple du DES, ces opérations sont les suivantes KEY PERM, exécutée en début de DES et SHIFT et COMP PERM exécutées à chaque tour. Lors de ces opérations, à certains moments, le microprocesseur manipule séparément un bit de la clé secrète, laissant donc la possibilité d'une attaque DPA sur ce bit.

On applique alors le procédé de contre-mesure selon l'invention en protégeant la donnée, la clé secrète en l'occurrence, avant d'effectuer ces opérations, en sorte qu'il n'est plus possible d'obtenir une information par attaque DPA.

Ainsi, et comme schématiquement représenté sur la figure 5, on tire une valeur aléatoire d'une première

donnée aléatoire Y, de même taille que la clé secrète K. On calcule une deuxième donnée aléatoire Z de même taille, en faisant un OU exclusif entre la clé secrète K et la première donnée aléatoire Y : $Z = K \text{ XOR } Y$.

5 Dans l'exemple, la séquence d'opérations comprend les opérations suivantes KEY PERM, SHIFT, COMP PERM. On applique alors cette séquence d'opérations sur chacune des deux données aléatoires Y et Z, successivement. Ainsi, à partir de ces deux données Y
10 et Z appliquées successivement en entrée, on obtient successivement les données Y' , $P_{1Y'}$, $K_{1Y'}$, respectivement Z' , $P_{1Z'}$, $K_{1Z'}$, en sortie des opérations KEY PERM, SHIFT, COMP PERM..

15 Un exemple pratique d'application au DES est représenté sur la figure 7.

Dans le DES, l'opération KEY PERM n'est exécutée qu'une seule fois, au début, tandis que la séquence d'opérations SHIFT et COMP PERM est exécutée dans chaque tour.

20 En outre, la sortie de l'opération SHIFT d'un tour T_i est appliquée comme entrée de l'opération SHIFT du tour suivant T_{i+1} (voir figures 1 et 2).

Pour appliquer le procédé de contre-mesure selon le deuxième mode d'application à cet algorithme DES, on
25 applique alors la première opération KEY PERM sur les données aléatoires Y et Z, ce qui donne deux données aléatoires intermédiaires, notées Y' et Z' . Ces deux données aléatoires intermédiaires sont successivement appliquées à l'opérations SHIFT du premier tour T_1 ,
30 fournissant deux données aléatoires intermédiaires notées $P_{1Y'}$ et $P_{1Z'}$. Ces deux données aléatoires sont d'une part mémorisées en mémoire de travail pour l'opération SHIFT du tour suivant (le deuxième tour),
35 et d'autre part appliquées successivement à l'opération EXP PERM du premier tour, pour fournir un premier résultat intermédiaire $K_{1Y'}$ et $K_{1Z'}$.

On procède ainsi dans chaque tour. Ainsi, à chaque tour T_i , on obtient un premier résultat aléatoire :

$K_{iy}' = \text{EXP PERM} (\text{SHIFT} (Y'))$;

et un deuxième résultat aléatoire :

5 $K_{iz}' = \text{EXP PERM} (\text{SHIFT} (Z'))$;

et les données aléatoires intermédiaires $\text{SHIFT} (Y') = P_{iy}'$ et $\text{SHIFT} (Z') = P_{iz}'$ sont mémorisées en mémoire de travail pour le tour suivant T_{i+1} .

10 Pour chaque tour T_i , on pourrait alors recalculer la sous-clé correspondante K_i correspondant à la séquence d'opérations KEY PERM, SHIFT et COMP PERM de ce tour appliquée à la clé secrète K , en faisant un OU exclusif entre les deux résultats aléatoires K_{iy}' et

15 K_{iz}' : $K_i = K_{iy}' \text{ XOR } K_{iz}'$.

Mais de préférence et comme représenté sur la figure 7, on ne recalcule pas la sous-clé K_i du tour T_i . On applique le premier résultat aléatoire K_{iy}' à la place de la sous-clé K_i dans une opération de OU exclusif XOR avec la donnée l fournie par l'opération d'expansion permutation EXP PERM. On obtient un

20 résultat intermédiaire b' .

En effectuant ensuite un OU exclusif XOR de ce résultat intermédiaire b' avec le deuxième résultat aléatoire K_{iz}' , on retrouve la donnée de sortie $b = \text{XOR} (l, K_i)$. On effectue donc les opérations

25 suivantes dans chaque tour T_i , pour calculer le paramètre b à partir de l :

$b' = l \text{ XOR } K_{iy}'$ et

30 $b = b' \text{ XOR } K_{iz}'$, comme représenté pour les premier et deuxième tours sur la figure 7.

De cette manière, on n'utilise plus la sous-clé secrète elle-même dans le calcul du message chiffré, mais des "sous-clés aléatoires": la clé se trouve donc

35 protégée avant et pendant l'exécution de l'algorithme cryptographique, car K_{iy}' et K_{iz}' étant aléatoires et

non connues du monde extérieur du composant (ou de la carte), elles sont susceptibles de changer à chaque nouvelle exécution de l'algorithme de cryptographie. On notera que dans l'application du procédé de contre-
5 mesure selon l'invention au calcul et à l'utilisation des sous-clés, on tire une seule fois une valeur aléatoire, en début d'exécution de l'algorithme, avant les opérations sur la clé secrète.

Ce deuxième mode d'application du procédé de
10 contre-mesure selon l'invention à la clé secrète peut être avantageusement combiné avec le premier mode d'application du procédé de contre-mesure au calcul du message chiffré proprement dit, cette combinaison rendant particulièrement efficace la contre-mesure.

15 La présente invention s'applique à l'algorithme de cryptographie à clé secrète DES, pour lequel des exemples de mise en oeuvre ont été décrits. Il s'applique plus généralement à tout algorithme de cryptographie à clé secrète dont l'exécution par le
20 microprocesseur de certaines opérations nécessitent une manipulation bit par bit de données.

Un composant électronique 1 mettant en oeuvre un procédé de contre-mesure selon l'invention dans un algorithme de cryptographie à clé secrète DES, comprend
25 typiquement, comme représenté sur la figure 8, un microprocesseur oP, une mémoire programme 2 et une mémoire de travail 3. Des moyens 4 de génération d'une valeur aléatoire, sont prévus qui, si on se reporte aux organigrammes des figures 3 et 5, fourniront les
30 valeurs aléatoires U et/ou Y de la taille voulue (32 bits pour U, 64 bits pour Y) à chaque exécution de l'algorithme de cryptographie. Un tel composant peut tout particulièrement être utilisé dans une carte à puce 5, pour améliorer son inviolabilité.

REVENDECATIONS

1. Procédé de contre-mesure contre des attaques par analyse différentielle de consommation de courant dans un composant électronique mettant en oeuvre un algorithme cryptographique à clé secrète K sur un message d'entrée (M), caractérisé en ce que l'exécution d'une opération (OPN) ou d'une séquence d'opérations comprenant une manipulation bit par bit d'une donnée d'entrée (D), pour fournir une donnée de sortie (OPN(D)), comprend les étapes suivantes :

- tirage d'une valeur aléatoire, d'une première donnée aléatoire (U), de même taille que la donnée d'entrée (D);

- calcul d'une deuxième donnée aléatoire (V), en effectuant un OU exclusif entre la donnée d'entrée et la première donnée aléatoire (U);

- exécution de l'opération (OPN) ou de la séquence d'opération successivement à la première donnée aléatoire (U) et à la deuxième donnée aléatoire (V), fournissant respectivement un premier résultat aléatoire (OPN(U)) et un deuxième résultat aléatoire (OPN(V)) ;

- calcul de la donnée de sortie (OPN(D)) en effectuant un OU exclusif entre lesdits premier et deuxième résultats aléatoires.

2. Procédé de contre-mesure selon la revendication 1, caractérisé en ce qu'il est appliqué à des opérations (EXP PERM, P PERM) portant sur des données calculées à partir du message d'entrée (M).

3. Procédé de contre-mesure selon l'une quelconque des revendications précédentes, caractérisé en ce que

l'on tire une nouvelle valeur aléatoire (U) à chaque nouvelle exécution de la dite opération ou séquence d'opérations.

5 4. Procédé de contre-mesure selon la revendication 1, appliqué à une opération ou une séquence d'opérations (KEY PERM, SHIFT, COMP PERM) effectuées sur ladite clé secrète K.

10 5. Procédé de contre-mesure selon la revendication 4, l'algorithme de cryptographie comprenant plusieurs tours de calcul, et comprenant une séquence d'opérations sur la clé secrète K pour fournir, à chaque tour (T_i), une sous-clé correspondante (K_i),
15 procédé caractérisé en ce qu'il est appliqué à ladite séquence d'opérations pour fournir, à chaque tour, un premier résultat aléatoire ($K_{iy'}$) et un deuxième résultat aléatoire ($K_{iz'}$).

20 6. Procédé de contre-mesure selon la revendication 5, chaque tour (T_i) une opération de OU exclusif entre la sous-clé (K_i) et une donnée d'entrée (l) pour fournir une donnée de sortie (b), caractérisé en ce que cette opération est remplacée par les opérations
25 suivantes :

 - calcul du OU exclusif entre ladite donnée d'entrée (l) et le premier résultat aléatoire ($K_{iy'}$) pour fournir un résultat intermédiaire (b');

 - calcul du OU exclusif entre ledit résultat
30 intermédiaire (b') et le deuxième résultat aléatoire ($K_{iz'}$) pour fournir ladite donnée de sortie (b).

 7. Procédé de contre-mesure selon l'une quelconque des revendications 1, 2, 3, 5, et 6, caractérisé en ce
35 que l'on tire une nouvelle valeur aléatoire (U ou Z) à

chaque nouvelle exécution de l'algorithme de cryptographie.

5 8. Procédé de contre-mesure selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il est appliqué à l'algorithme DES.

10 9. Composant électronique de sécurité mettant en oeuvre le procédé de contre-mesure selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend des moyens (4) de génération d'une valeur aléatoire, un microprocesseur (oP), une mémoire programme (2) et une mémoire de travail (3), lesdits
15 moyens (4) fournissant au moins une valeur aléatoire (U) et/ou (Y) de la taille voulue, 32 bits pour (U) et 64 bits pour (Y), à chaque exécution de l'algorithme de cryptographie.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference GEM0630	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/FR00/00130	International filing date (day/month/year) 20 January 2000 (20.01.00)	Priority date (day/month/year) 17 February 1999 (17.02.99)
International Patent Classification (IPC) or national classification and IPC H04L 9/06		
Applicant GEMPLUS		

- This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
- This REPORT consists of a total of 8 sheets, including this cover sheet.
☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 25 sheets.

- This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability: citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand 14 September 2000 (14.09.00)	Date of completion of this report 22 May 2001 (22.05.2001)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR00/00130

I. Basis of the report

1. With regard to the **elements** of the international application:*

- ☐ the international application as originally filed
- ☒ the description:
 pages _____, as originally filed
 pages _____, filed with the demand
 pages 1-15, filed with the letter of 09 March 2001 (09.03.2001)
- ☒ the claims:
 pages _____, as originally filed
 pages _____, as amended (together with any statement under Article 19
 pages _____, filed with the demand
 pages 1-9, filed with the letter of 09 March 2001 (09.03.2001)
- ☒ the drawings:
 pages _____, as originally filed
 pages _____, filed with the demand
 pages 1/7-7/7, filed with the letter of 09 March 2001 (09.03.2001)
- ☐ the sequence listing part of the description:
 pages _____, as originally filed
 pages _____, filed with the demand
 pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language _____ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR00/00130

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

1. The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non obvious), or to be industrially applicable have not been examined in respect of:

☐ the entire international application.

☒ claims Nos. 6.9

because:

☐ the said international application, or the said claims Nos. _____
relate to the following subject matter which does not require an international preliminary examination (*specify*):

☒ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. 6.9
are so unclear that no meaningful opinion could be formed (*specify*):

See supplemental sheet

☐ the claims, or said claims Nos. _____ are so inadequately supported
by the description that no meaningful opinion could be formed.

☐ no international search report has been established for said claims Nos. _____

2. A meaningful international preliminary examination cannot be carried out due to the failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions:

☐ the written form has not been furnished or does not comply with the standard.

☐ the computer readable form has not been furnished or does not comply with the standard.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR 00/00130

Supplemental Box

(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: III.

See Box VIII regarding Claims 6 and 9.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR 00/00130

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-5, 7-8	YES
	Claims		NO
Inventive step (IS)	Claims	1-5, 7-8	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-5, 7-8	YES
	Claims		NO

2. Citations and explanations

I

The following documents (D) have been taken into account when establishing the preliminary examination report:

D1: NTT REVIEW, vol. 6, no. 4, 1 July 1994, pages 85-90, MIYAGUCHI S: "SECRET KEY CIPHERS THAT CHANGE THE ENCIPHERMENT ALGORITHM UNDER THE CONTROL OF THE KEY", XP000460342.

D2: INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, PHOENIX, ARIZONA, NOV. 3-8, 1997, vol. 2, 3, 3 November 1997, pages 689-693, YI X ET AL: "A METHOD FOR OBTAINING CRYPTOGRAPHICALLY STRONG 8 X 8 S-BOXES", XP000737626

D3: FR-A-2 762 402

II

The present invention relates to a countermeasure

method to be used against differential power analysis (DPA) attacks in an electronic component using a secret key cryptographic algorithm.

There are numerous secret key algorithms which can only be run by the microprocessor carrying out, at certain times, bit-by-bit data manipulation operations. In particular, algorithms generally include permutations requiring such manipulation operations by the microprocessor.

By analysing power consumption during said bit-by-bit data manipulation operations, the value of at least a few of the manipulated data bits can be recovered. Such information regarding the data may provide further information relating to intermediate results obtained when executing the encryption algorithm, which can lead, in turn, to the recovery of at least a portion of the bits of the secret key used.

The present invention aims to protect the data undergoing bit-by-bit manipulation by applying a countermeasure, i.e. a scrambling procedure, so that the analysis of power consumption during the data manipulation operation does not disclose any information regarding said data. For each operation or series of operations applied to input data, and including at least one bit-by-bit manipulation operation, the invention comprises the steps of initially drawing a first random data identical in size to the first data, calculating a second random data by carrying out an exclusive OR operation between the first random data and the input data, and sequentially applying said operation or series

of operations to the first random data and to the second random data. In this way, said operation or series of operations only manipulates random data, so that it is no longer possible to carry out a differential power analysis attack. Recovering the output data corresponding to the series of steps carried out on the input data simply involves calculating the exclusive OR between the first and second random results.

Document D1 relates to a solution to a mathematical problem whereby known encrypted message attacks can be avoided. The method described includes modifying the subpart of the key in the algorithm, for any secret key algorithm. The technology described in said document includes data rotation as well as data substitution operations.

Thus, the present invention differs from document D1 in that it does not modify the structure of the algorithm, nor the data input or output thereof. The XOR operation used allows data to be masked by means of a random parameter.

Document D2 concerns a proposition for improving S BOXES in the standard DES algorithm in order to enhance protection at the cryptanalytical level, i.e. in mathematics, but not in physical cryptography.

The invention also differs from document D2 in that it addresses physical cryptography problems, i.e. it proposes a solution to implementation problems involving the occurrence of side effects; moreover, it does not relate to S BOXES but addresses

protection problems arising in the course of data compression, permutation and expansion operations.

Document D3 concerns a method and a device using the standard DES algorithm to produce a random number generator. Said DES algorithm is a secret key algorithm including data, such as a counter for generating an output result that may be assimilated to a random number, said result being located outside the DES.

The invention differs from document D3 in that it uses a random number within the DES algorithm to protect the execution thereof against all types of attacks.

An inventive step is therefore recognised. Claims 1-5 and 7-8 therefore meet the requirements of PCT Article 33(3).

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. The grammatical structure of Claim 6 is not clear (PCT Article 6): the first sentence does not include a verb. Does the applicant intend to state that "every time an exclusive OR operation between the sub-key and an input data **is run**, said operation is replaced by the following data ..."?

2. Claim 9 is unclear (PCT Article 6) in that it mentions that a random value is generated, but does not mention what is thereafter done with said random variable (calculating a second random data, carrying out an operation, calculating an output data, etc...).

Surely, the invention does not simply include generating a random variable, but resides rather in the means for using said variable to respond to DPA attacks.

The device claim is therefore unclear in that it does not include all the essential technical features required to define the invention (PCT Article 6, in combination with PCT Rule 6.3(b)).

Moreover, the wording "of a desired size" is a relative expression and has no specific meaning (see PCT Guidelines, Chapter III-4.5).

3. Claims 5 and 6 are unclear in that the wording "characterised in that" does not immediately follow "Method... as per Claim...". These two claims are indirectly dependent on Claim 1, which already

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR 00/00130

VIII. Certain observations on the international application

contains a preamble and a characterising portion.
Claims 5 and 6, combined with Claim 1, therefore
have two preambles and two characterising portions,
thereby casting a doubt on the scope of protection
thereof.